A METHOD OF ENABLING A MULTITASKING COMPUTING DEVICE TO CONSERVE RESOURCES

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates to a method of enabling a multitasking computing device to preserve or conserve resources, such as battery power. The term 'computing device' used in this patent specification should be expansively construed to cover any kind of computing device and includes without limitation radio telephones, smart phones, communicators, personal computers, lap top computers, game consoles, computers and application specific devices.

2. Description of the Prior Art

Battery conservation in battery operated computing devices is very important, particularly in devices such as smartphones that consume high power levels by virtue of connecting to always-on GPRS or 3G cellular networks.

In conventional multi-tasking computers running several different applications at the same time, an application will issue a software interrupt to the operating system when it first requests services; interrupts from different applications are prioritised and queued by an interrupt handler. A scheduler starts and ends applications and manages concurrently running applications.

Conventionally, the scheduler will end an application when instructed to do so by the end user, e.g. selecting a 'close' option in the application's drop down menu. Consequently, without an explicit 'close' command, applications will continue to run even when not actually in active use; they will therefore continue to use some system resources, even when residing in the 'background'. An application is in the background if it is not being interacted with by an end-user and it presents no user interface with which a user could interact (but it could for example present an icon indicating its

presence and the fact that it was still active). A foreground application conversely does present a user interface with which a user can interact.

Hence, the problem of battery conservation is especially acute for multi-tasking devices, i.e. devices with an operating system that can run several applications at the same time.

SUMMARY OF THE INVENTION

In a first aspect of the present invention, a multitasking computing device determines if a non-trusted application is in the background or foreground and prevents an untrusted application that is in the background from running in order to preserve system resources.

It is valuable to preserve system resources (CPU, power) in multitasking computing devices: For mains powered desktop computers, the fact that applications can run in the background and hence still consume some system resource is a waste of CPU and scheduler activity. And in the battery operated, portable device domain, it is especially valuable to conserve system resources wherever possible since doing so can increase battery life, as noted earlier.

A device implementing the present invention preserves system resources by denying system resources and services to background applications that do not meet predefined 'trust' or certification criteria – i.e. criteria which define the level of trustworthiness of the application. There are various criteria that may be relevant in assessing whether a give application is 'untrusted' or not; these include, without limitation:

(a) which protected resources on the device can be accessed by the application: an 'untrusted' application might be defined as one that is not able to access certain predefined protected resources; or

(b) whether the application was loaded from ROM or RAM: applications loaded from RAM are likely to be from third party sources and hence less trustworthy than applications loaded from ROM, which would typically be provided by the device manufacturer; or

(c) whether the application has been validated using some predefined validation or certification process.

Applications might, in theory, be written so that they take notice of an event sent to them when they are sent to background, causing them to automatically cease running. But even this is likely to be missed in applications which are from certain kinds of third party programmers or are not validated as proper implementations – i.e. 'untrusted' applications. 'Untrusted' applications are therefore more likely to contain a wrong implementation of normal background behaviour: hence, merely relying on an

application to voluntarily cease running when notified that it is in the background is an inadequate strategy for untrusted applications. Instead, they need to be actively prevented from running.

With the present invention, untrusted third party applications (such as downloaded applications like games) are prevented from running in the background and are suspended. Trusted applications may still be allowed to run in the background, or they may be actively prevented in the same way as non-trusted applications, or they may be requested (but not prevented) to stop running if in background. Trust will conventionally be established for a given application using a signature in the application installation file, although there are other techniques that may be deployed as part of the secure computing base of the device.

In a second aspect, there is a multitasking computing device programmed to be capable of determining if an untrusted application is in the background or foreground and preventing an untrusted application that is in the background from running in order to conserve system resources. The device may be battery powered.

In a third aspect, there is an operating system for a multitasking computing device, the operating system being capable of determining if an untrusted application is in the background or foreground and preventing an untrusted application that is in the background from running in order to conserve system resources.

BRIEF DESCRIPTION OF THE DRAWING

The invention will be described with reference to the accompanying drawing, which is a schematic of some of the components of a device in accordance with the present invention.

DETAILED DESCRIPTION

The present invention can be implemented on battery operated devices running SymbianOS operating system. SymbianOS based phones are 'open' for third party applications. The third party applications are often games or similar types of applications and, when these execute, the CPU is often running at full speed to update graphics, sounds etc. When the user or the system needs to display another application or dialog, there is a risk that the third party application will still run in the background and thus drain the battery.

Third party applications can either come from 'trusted' sources or 'untrusted' sources. This may be determined by a signature in the installation file. An alternative approach to platform security on SymbianOS is described in PCT/GB2003/002311, the contents of which are incorporated by reference.

With the present invention, when an untrusted application is running on the battery operated device and another application should be in the foreground, the untrusted application is placed into the background and is also actively prevented from running. This denies it system resources and hence preserves power, as well as unnecessary CPU activity associated with the untrusted application in background. Preserving system resources could be especially valuable not only in the context of portable, battery powered devices, but also a UPS (uninterruptible power supply) powered system: once activated because a primary power source has ceased to provide power, the need to preserve system resources for as long as possible is very valuable. When the untrusted application is brought to the foreground again, it is allowed to run again.

The scheme is implemented by a system component which both knows which processes and threads belong to trusted or untrusted applications as well as knows which application is in foreground and which ones are in background. In Symbian OS, this is most likely to be the window server component. C++ and Java applications can also be controlled in this way.

Referring now to **Figure 1**, a window server component **2** is used to determine if an application is in the background or foreground on display **1**; for an untrusted application

4 in the background, it can send a control signal to the scheduler 3 or interrupt handler that in effect prevents the untrusted application 4 from running, e.g. being given any services or consuming any resources. The scheduler could for example, simply operate so as to never allocate any services or resources to the background untrusted application 4; an alternative would be for the interrupt handler to simply place any interrupts from the background untrusted application 4 to the back of its queue and never allow them to be executed. When in the background, trusted application 5 may continue to run, or may be actively prevented in the same way as non-trusted application 4, or may be requested (but not prevented) to stop running.

One example use of the present invention is to prevent background untrusted applications from 'polling' for data over a wireless network, an activity that can potentially drain a battery quickly. Another example is that untrusted applications will automatically be prevented from running if the display shows a screen saver or is actually turned off (battery operated devices can perform useful functions such as telephony even when the screen is turned off). Hence, the present invention is a valuable addition to power conservation strategies, especially (although without limitation) to battery operated devices.

When the device determines that an application is in the foreground (again, as may be determined by a window server component), it allows that application to run again – e.g. to be provided with resources and services.

CLAIMS

1. A method of enabling a multitasking computing device to preserve system resources, comprising the steps of determining if an untrusted application is in the background or foreground and preventing an untrusted application that is in the background from running.

2. The method of Claim 1 in which a window server component determines if the untrusted application is in the background or foreground.

3. The method of Claim 2 in which, for an untrusted application in the background, the window server sends a control signal to a scheduler or interrupt handler to prevent the application from running.

4. The method of Claim 1 comprising the further step of preventing an untrusted background application from 'polling' for data over a wireless network.

5. The method of Claim 1 comprising the further step of preventing an untrusted background application from running if a display shows a screen saver or is turned off.

6. The method of Claim 1 in which a trusted application in the background is (i) still allowed to run, or (ii) actively prevented from running or (iii) requested to stop running .

7. The method of Claim 1 in which an application has been deemed to be untrusted by the device assessing:

(a) which protected resources on the device can be accessed by the application; or

(b) whether the application was loaded from ROM or RAM; or

(c) whether the application has been validated using some predefined validation or certification process.

8. The method of Claim 7 in which a background application is prevented from running only if it does not meet predefined 'trust' or certification criteria established using a signature in an installation file for the application.

9. The method of Claim 1 in which the device is battery powered.

10. The method of Claim 1 in which the system resources that are preserved are one or more of (i) power, (ii) CPU activity and (iii) scheduler activity.

11. The method of Claim 1 in which the device is powered by a UPS (uninterruptible power supply).

12. A multitasking computing device programmed to be capable of determining if an untrusted application is in the background or foreground and preventing an untrusted application that is in the background from running in order to conserve system resources.

13. The device of Claim 11 which is battery powered.

14. An operating system for a multitasking computing device, the operating system being capable of determining if an untrusted application is in the background or foreground and preventing an untrusted application that is in the background from running in order to conserve system resources.

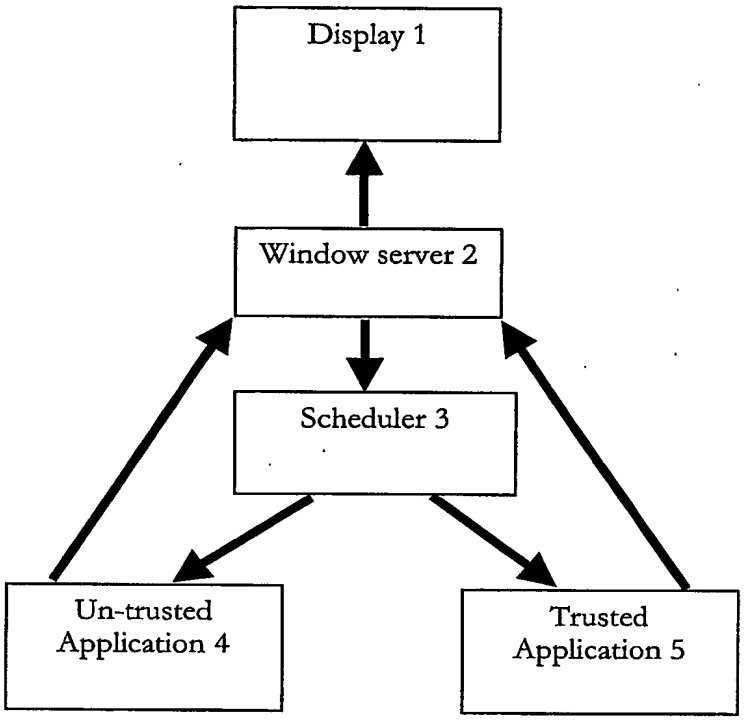
Display 1
Window server 2
Scheduler 3
Un-trusted Application 4
Trusted Application 5

Figure 1

INTERNATIONAL SEARCH REPORT

International Application No
../GB2004/002912

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F9/46 G06F1/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	HASSLER V ET AL: "Controlling applets' behavior in a browser" COMPUTER SECURITY APPLICATIONS CONFERENCE, 1998. PROCEEDINGS. 14TH ANNUAL PHOENIX, AZ, USA 7-11 DEC. 1998, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 7 December 1998 (1998-12-07), pages 120-125, XP010318612 ISBN: 0-8186-8789-4 paragraph '0001! paragraph '0002! paragraph '02.2! paragraph '0003! - paragraph '03.2! -/--	1-14

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 November 2004	10/12/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Kusnierczak, P

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
GB2004/002912

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	"RWsSession in Window Server" 'Online! 2002, SYMBIAN , XP002306026 Retrieved from the Internet: URL:http://www.symbian.com/developer/techlib/v70docs/sdl_v7.0/doc_source/reference/cpp/WindowServerClientSide/RWsSessionClass.html> the whole document	1-14
A	EP 0 942 368 A (LUCENT TECHNOLOGIES INC) 15 September 1999 (1999-09-15) paragraph '0014! - paragraph '0021! paragraph '0024! - paragraph '0053!	1-14
A	WO 01/04743 A (SUN MICROSYSTEMS INC) 18 January 2001 (2001-01-18) page 3, line 16 - page 5, line 15 page 8, line 3 - line 22 page 9, line 16 - page 18, line 22	1-14
A	SCHMID M ET AL: "Preventing the execution of unauthorized win32 applications" IEEE, vol. 2, 12 June 2001 (2001-06-12), pages 175-183, XP010548745 paragraph '0001! - paragraph '03.5!	1,5-8, 12,14

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
GB2004/002912

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0942368 A	15-09-1999	US 6260150 B1	10-07-2001
		CN 1233015 A	27-10-1999
		EP 0942368 A2	15-09-1999
		JP 11296388 A	29-10-1999
WO 0104743 A	18-01-2001	AU 5934500 A	30-01-2001
		AU 6097300 A	30-01-2001
		AU 6099200 A	30-01-2001
		AU 776813 B2	23-09-2004
		AU 6349500 A	30-01-2001
		CA 2373036 A1	18-01-2001
		CA 2378588 A1	18-01-2001
		CA 2378844 A1	18-01-2001
		CN 1360694 T	24-07-2002
		CN 1360695 T	24-07-2002
		CN 1373967 T	09-10-2002
		EP 1194838 A2	10-04-2002
		EP 1194840 A2	10-04-2002
		EP 1192617 A1	03-04-2002
		EP 1197090 A2	17-04-2002
		JP 2003504923 T	04-02-2003
		JP 2003504753 T	04-02-2003
		JP 2003504754 T	04-02-2003
		JP 2003522442 T	22-07-2003
		WO 0104743 A2	18-01-2001
		WO 0104868 A1	18-01-2001
		WO 0104744 A2	18-01-2001
		WO 0105158 A1	18-01-2001
		US 6701334 B1	02-03-2004
		US 6762798 B1	13-07-2004